

OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 20

June 27, 2006

APPROVED BY THE BOARD OF POLICE COMMISSIONERS ON JUNE 6, 2006

**SUBJECT: TRAINING EVALUATION AND MANAGEMENT SYSTEM (TEAMS) -
EXPANDED**

PURPOSE: The Consent Decree mandated a number of changes to Department operating practices. One of the mandated changes was the expansion of the Training Evaluation and Management System (TEAMS) to promote professionalism and best policing practices while encouraging appropriate employee mentoring. Consequently, TEAMS was enhanced to become TEAMS II with the addition and modification of several databases, an ability to receive, organize and store data from 14 information databases, an ability to complete on-line reports/investigations, and an ability to perform complex employee and organizational performance analyses.

While TEAMS II stores data from a number of specific databases and allows for a "drill down look" at specific records associated with a specific performance entry, it is the Risk Management Information System (RMIS) that collects selected performance data, identifies connecting reports, and performs analytical performance comparisons with corresponding notices.

Office of the Chief of Police Notice, dated July 10, 1997, *Training Evaluation and Management System (TEAMS) Department - Wide Implementation*, implemented TEAMS and established the initial usage and access guidelines. Special Order No. 13, dated April 5, 2002, *Training Evaluation and Management System Guidelines*, refined those guidelines and is summarized in Department Manual Section 1/668. This Order updates Department Manual Section 1/668 by renaming TEAMS as TEAMS II, identifying the nature of on-line reporting, and reinforces the existing TEAMS usage and access protocols.

PROCEDURE:

I. TRAINING EVALUATION AND MANAGEMENT SYSTEM II (TEAMS II) - ESTABLISHED. The expanded Training Evaluation and Management System (TEAMS) is now known as TEAMS II and is composed of the following:

A. Contributing Source Systems. The following databases contribute selected data to TEAMS II:

- * Canine System (K-9)
- * Claims/Lawsuit Information System (CLIS)
- * Complaint Management System (CMS)
- * Comprehensive Automated Permit System (CAPERS)
- * Consolidated Crime Analysis Database (CCAD)
- * Department Employees Commendation System (DECS)
- * Deployment Period System (DPS)
- * Fleet Safety Reporting (FSR)
- * Shooting Qualification and Bonus System (SQUABS)
- * System to Organize Pedestrian/Vehicle Stops (STOPS)
- * Traffic Information System (TIS)
- * Training Management System (TMS)
- * Use of Force System (UOFS)
- * Vehicle Pursuit System (VPS)

B. Risk Management Information System (RMIS). RMIS is comprised of selected data from the source systems. The system performs analytical comparisons, threshold evaluations, and cross-referencing. It also prepares reports and produces action items and notifications.

C. Access Control. TEAMS II shall provide common access functionality and shall be strictly regulated through the Access Control System, which also gives the Department the ability to perform on-line reporting.

II. USE OF TEAMS II. The guidelines and protocols currently used for TEAMS remain applicable to TEAMS II. Whereas TEAMS was a "pointer" system used predominantly to generate a complete or modified personnel summary report, TEAMS II is a "pointer" system to be used not only to obtain a personnel summary report, but to identify those employees and organizational entities whose performance is well outside that of their respective peer group average, and encourage appropriate supervisory recognition or mentoring.

It is the responsibility of managers and supervisors to regularly review an employee's personnel file and other documents, which are the source documents for a TEAMS II entry. It is only from actual review of such documents that a conclusion may be made as to whether or not a problem exists and what, if anything, should be done. In no case shall a TEAMS II report be used as a substitute

for an employee's personnel file or any other document(s), which is the source for a TEAMS II entry.

A. TEAMS II Employee Summary Report. The TEAMS II Employee Summary Report contains personnel summary information. Currently, a TEAMS II Employee Summary Report includes the following personnel information categories:

- * Arrest/Crime Reports summary
- * Attendance data summary
- * Citations data summary
- * Civil Litigation data summary
- * Major and Minor Commendations summary
- * Discipline data summary
- * In-Service Training Courses summary
- * Pursuit data summary
- * Rank/Assignment summary
- * STOPS data summary
- * Traffic Collisions data summary
- * Use of Force (all) data summary
- * Work Permit data summary

An inquiry to obtain a TEAMS II Employee Summary Report will not only provide summary data, but will also allow the operator to select a specific entry and view associated reports in RMIS and in the case of UOF or complaints, the completed investigation.

Note: Attendance data will not be displayed on the initial Teams II Employee Summary Reports; it will be added in the future.

B. TEAMS II Performance Assessment. Individual performance assessments are accomplished using the new Teams II Summary Report and the appropriate RMIS Reports.

III. TYPES OF TEAMS II REPORTS.

A. TEAMS II Employee Summary Reports. TEAMS II Employee Summary Reports will continue to be produced in multiple versions or "views" based on how the report is to be used. These versions or "views" differ only in the manner in which information about personnel complaints will be displayed on the report. Attachment No.1, "TEAMS

Filters used to determine when a complaint is displayed on a TEAMS Report," has been updated and includes the following new versions or "views" of the report:

1. Risk Management Executive Committee (RMEC) Profile Review.
2. Professional Standards Bureau (PSB)/Force Investigation Division (FID)/Office of Inspector General (OIG) Review.
3. Risk Management Information System Threshold View.

B. OTHER REPORTS. TEAMS II will also provide a number of standardized reports that provide a summary of an employee's performance in comparison to their peer group, their co-workers, watch, division, area, bureau, etc. There are similar reports for supervisors as well as organizational comparisons.

IV. AUTHORIZED ACCESS. Access to TEAMS II remains as specified in Department Manual Section 1/668.

V. ACCESS AND PROXY DELEGATION. TEAMS II has the ability to allow an authorized user to delegate access rights to other users depending upon the employee's rank, pay grade, organization, function, and duty assignment. Delegation of access rights is the process of limiting or permitting a user's access to various RMIS reports and information. Proper delegation of access rights ensures that each user can only access information to which that user has a right and a need to know.

An authorized user may also delegate proxy rights to a subordinate that allows the subordinate to act for the authorized user. This includes approving reports such as Use of Force reports, action items, and complaints that require a commanding officer's signature for approval. A commanding officer can give proxy rights to their assistant commanding officer or a member of their staff such as an adjutant, who could then sign off for the commanding officer, when he/she is not available to access the system and has at least verbally approved the report. Granting proxy rights shall be closely monitored by a commanding officer and should be rarely used.

A commanding officer is responsible for the actions taken by their proxy. The system will always record the name of the actual person taking the action if the approval is by an authorized proxy, similar to signing your name with the word "for" over the signature block of another person on paper documents.

Access control is dependant upon the DPS system and it is critical that all commands keep the DPS up to date. Access and proxy delegation may only be made to personnel within the delegating person's chain of command, where the delegated rights will remain in effect until one of the following occurs:

- * The status of the employee changes, (e.g., transfer, change in rank, or resignation);
- * The status of the person delegating changes (e.g., transfer, change in rank, resignation);
- * The matter requiring the delegated access was completed (e.g., a captain delegated their access rights to their adjutant to complete a specific project generated by the TEAMS II system. Upon completing the project, the adjutant reverts back to their personal access rights); or,
- * Risk Management Group rescinds the access rights.

VI. RESPONSIBILITY FOR MAINTAINING TEAMS. The Department entities responsible for the data entry/maintenance of the specific categories are as follows:

<u>CATEGORY</u>	<u>RESPONSIBLE DEPARTMENT ENTITY</u>
Arrest/Crime Reports	Record & Identification Division
Attendance	Fiscal Operations Division
Citations	Information Technology Division
Civil Litigation	Risk Management Group
Commendations-Major	Personnel Group
Commendations-Minor	Employee's Command
Discipline	Internal Affairs Group

In-Service Training	Training Division
Pursuits	Risk Management Group
Rank/Assignment	Personnel Division
STOPS	Civil Rights Integrity Division
Traffic Collision	Special Operations Support Division
Use of Force (All)	Use of Force Review Division
Work Permit	Personnel Group

A. Entering Data. The Department entity responsible for maintaining information used by TEAMS II shall ensure that any new or revised data is entered into the appropriate system within 30 days of receiving the information.

B. Correcting Data. The procedure to correct TEAMS II data remains the same as required by Department Manual Section 3/791.

VII. PROCEDURE TO DISPUTE INFORMATION CONTAINED IN TEAMS II.

The procedure to dispute information contained in TEAMS II remains the same as required by Department Manual Section 3/791.

VIII. CONFIDENTIALITY OF TEAMS II INFORMATION. Although computerization makes TEAMS II data more readily available, it is critical that each employee understands the confidential nature of such information. **Breaches of such confidentiality will not be tolerated.**

The information contained in TEAMS II is confidential personnel information and should be treated as such. The fact that this information is accessible to certain select individuals on a "NEED TO KNOW/RIGHT TO KNOW" basis does not diminish the confidential nature of this material. Because it may contain information obtained from police officer personnel records concerning discipline, use of force, attendance, medical information or injured on duty status, whether in cursory form or in

detail, said information is subject to protection as confidential personnel documents under Penal Code Sections 832.7, 832.8, Government Code Section 6254(C) and (G), Government Code Section 6255, and Article 1, Section 1 of the California Constitution, as well as Department Manual Section 3/405.

Note: TEAMS II contains a monitoring feature that allows managers to monitor an employee's access of TEAMS II data.

- IX. Information Technology Division's Responsibility.** The requirement for Information Technology Division to process TEAMS access authorization requests is rescinded. TEAMS II access control provides managers with the ability to delegate and restrict access authority based on the information maintained in the Deployment Period System.
- X. Risk Management Group's Responsibility.** Monitoring responsibilities assigned to Risk Management Group relative to TEAMS remains unchanged for TEAMS II.
- XI. Employees' Responsibility.** Employees are responsible for reviewing his/her TEAMS II Employee Summary Report to ensure the information is accurate and complete. Any discrepancies shall be brought to the attention of the appropriate entity, as established in this Order.
- XII. Supervisors' Responsibility.** Supervisors shall ensure that access rights to the TEAMS II/RMIS, which they have granted or delegated to other employees, has been done so only on a "NEED TO KNOW/RIGHT TO KNOW" basis. The TEAMS II query may contain information obtained from police officer personnel records concerning discipline, use of force, attendance, medical information or injured on duty status, whether in cursory form or in detail, said information is subject to protection as confidential personnel documents under Penal Code Sections 832.7, 832.8, Government Code Sections 6254(C), 6254(G), and 6255, and Article 1, Section 1 of the California Constitution, as well as Department Manual Section 3/405.
- XIII. Commanding Officers' Responsibility.** Commanding officers shall ensure that access rights to TEAMS II/RMIS have been granted or delegated to employees within their command only on a "NEED TO KNOW/RIGHT TO KNOW" basis.

Because this query may contain information obtained from police officer personnel records concerning discipline, uses of force, attendance, medical information or injured on duty status, whether in cursory form or in detail, said information is subject to protection as confidential personnel documents under Penal Code Sections 832.7, 832.8, Government Code Sections 6254(C), 6254(G), and 6255, and Article 1, Section 1 of the California Constitution, as well as Department Manual Section 3/405. Commanding officers shall ensure that access rights for all employees within their command are appropriately granted, delegated, revised, or rescinded. Commanding officers shall ensure supervisory personnel provide a TEAMS II Employee Summary Report to each employee in conjunction with the service of the employee's annual (post-probationary) Performance Evaluation Report.

AMENDMENTS: This Order amends Department Manual Section 1/668.

AUDIT RESPONSIBILITY. The Commanding Officer, Risk Management Group, shall monitor compliance with this directive in accordance with Department Manual Section 0/080.30.

WILLIAM J. BRATTON
Chief of Police

DISTRIBUTION "D"